

## ABSTRACT

In a quantum key distributing method according to the present invention, an error of reception data is corrected using check matrixes for an "Irregular-LDPC code" that are  
5 definite and have stable characteristics and a part of shared information is discarded according to error correction information laid open to the public. In addition, in the quantum key distributing method according to the present invention, a parity check matrix  
10 corresponding to a specific coding ratio is extracted from parity check matrix optimized at a coding ratio in a desired range while a coding ratio is lowered until the error of the reception data is completely corrected, an additional syndrome is generated, and error correction  
15 processing is repeatedly executed using the additional syndrome.